Table of Contents

List of Tables and Exhibits

1. INTRODUCTION

The Standard Procurement System (SPS) Infrastructure/Architecture Document describes the technical architecture of the SPS and the infrastructure on which the SPS will operate. The designed architecture supports a variety of anticipated configurations ranging from dial-in sites (with or without a local database), afloat or deployed units, stand-alone users, sites supporting users with local area network (LAN) and local servers, users located at regional Information Processing Centers (IPCs), and users located at Defense Megacenters (DMCs). The system architecture described here is the SPS design framework.

1.1 Purpose

This document provides the Procurement community with a technical reference including the definition of the SPS target architecture. This document describes the SPS application requirements, the existing environment, the target architecture, the handling of data within this architecture, and the infrastructure on which SPS operates. The defined target architecture and infrastructure incorporate the existing heterogeneous and evolving environment and facilitate the phased SPS implementation. This document also describes the SPS target architecture and infrastructure in relation to other Department of Defense (DoD) initiatives, such as the Defense Information Infrastructure (DII) and the Global Combat Support System (GCSS).

2. SPS APPLICATION

The SPS application guidance derives from the SPS contract released 23 August 1996. The application and its implementation within the SPS infrastructure must comply with the standards listed in Appendix D.

2.1 Architecture, Software, and Security Requirements

This section reviews the architecture, software, and security specifications of the SPS application. This document includes these requirements for reference and to increase the understanding of the SPS application within the defined infrastructure.

2.1.1 Target Architecture Requirements

The SPS application operates within the minimum requirements described in Section 5 and Appendix D. The application must operate in a variety of environments based on the configurations described in Section 3. These environments may include a stand-alone, non-dedicated environment without network connectivity; an environment with personal computers (PCs) networked to Portable Operating System Interface for Computer Environments (POSIX) compliant minicomputer and platform servers; and PCs and networks with varying levels of connectivity to the Defense Information Systems Network (DISN). The SPS architecture enables integration with the DMC databases in a client/server mode. The SPS contract states the SPS application must comply with guidelines in the Global Command and Control System (GCCS) Integration and Runtime Specification of August 1995 and the Global Command and Control

System Baseline Common Operating Environment of November 1994. The SPS application must comply with the Defense Information Infrastructure (DII) Common Operating Environment and the Implementation Plan for Global Combat Support System (GCSS) Initiative as well. Any end user interface must also be compatible with the Defense Message System (DMS) communications software, The entire system will need to meet certification requirements for the Federal Acquisition Computer Network. Section 6 describes the relation of the DII, GCSS, GCCS, and DMS to SPS.

2.1.2 Interface Requirements

All SPS software interfaces must comply with graphical user interface (GUI) standards for the host environment, concurrently perform or view multiple processes, allow multiple users to concurrently use an original document, report discrepant data or results, override system defaults, and allow remote users to access the system.

The SPS software must interface successfully with the centralized DoD database. The SPS interfaces to other systems external to SPS through data standardized in the Defense Data Dictionary System (DDDS) format. If data is not in a standard format, SPS provides translations.

In addition, the SPS software must comply with the American National Standards Institute (ANSI) X12 (3050 Implementation Convention or greater) standards for electronic data interchange (EDI). Compliance allows the SPS to extract or transmit data to any other government system that uses the X12 standards.

2.1.3 Security

The target SPS environment requires a security level C2, defined as business sensitive but unclassified. To maintain a C2 secure environment, the SPS software will provide discretionary access control, user identification and authentication, password encryption, auditing, and relevant documentation. Security must protect integrity, authenticity, availability, and privacy of all information created, processed, stored, and communicated within the SPS environment. The application level can impose security via operating system and database enforcement and controlling network communications between the various physical components of the collective SPS platform. Adequate security requires that security provisions placed at each level, on each component of the environment, and structured to complement the protections provided by every other level or component.

The SPS enforces security requirements using recommended security provisions provided by the National Security Agency (NSA). SPS security incorporates the Multilevel Information Systems Security Initiative (MISSI) and the FORTEZZA card. The MISSI provides the high-level strategy for security within the DII. The SPS software will protect system data through use of MISSI security products, including the FORTEZZA crypto card. The NSA, in conjunction with the Defense Information Systems Agency (DISA), developed the FORTEZZA-based solution to protect sensitive information against unauthorized disclosure through client/server security across open communication networks. With the FORTEZZA approach to secured communications, each authorized user possesses a cryptographic card containing embedded personal data. Each SPS client workstation requires a single FORTEZZA card reader (a Type II Personal Computer

Memory Card International Association (PCMCIA) slot). Each host server must read FORTEZZA encrypted data. Through the FORTEZZA card system, security services ensure data confidentiality, originator authentication, and data integrity.

FORTEZZA provides data security at an operational level that includes, but not limited to, data backup, control of user identification and passwords, data sensitivity/aggregation, and database access. User identification and password control include verification and authentication of a user's need to know, user's clearance, and user's date of authorized access as well as the authorization expiration date.

3. LEGACY ENVIRONMENT

Ten major systems function as contract placement or contract administration systems for the Army, Navy, Air Force, Marine Corps, and the Defense Logistics Agency (DLA). Contract automated information systems (AISs) include a mixture of two and three-tier architectures. The current environment suffers from fragmentation between several different legacy systems, each with a specific set of functions and deficiencies. Table 3-1 outlines typical configurations for the ten migration systems at the corporate, departmental, and personal tiers.

DoD Component	Legacy System	Corporate Tier	Departmental Tier	Personal Tier
Army	SAACONS		Unisys, Intel or Sequent	Unisys, Intel or Sequent, Dumb Terminals and Personal Computers
Army	CCSS/ PADDS	IBM	Unisys, Hewlett Packard	Personal Computers
Navy	APADE		Tandem	Personal Computers
Navy	ITIMP	Amdahl		Personal Computers Dumb Terminals
Air Force	AFMC	Data General Amdahl	AT&T	Dumb Terminals
Air Force	BCAS		AT&T, Wang	Dumb Terminals
Air Force	AMIS	Hitachi	Wang	Wang, Personal Computers
DLA	BOSS	IBM, Amdahl		Personal Computers
DLA	SPS/ DPACS	Hewlett Packard	Hewlett Packard	Zenith or Unisys, Personal Computers
DLA	SPS/ MOCAS	Amdahl	AT&T	Personal Computers Dumb Terminals

Table 3-1: Overview of As-Is Legacy Systems

These ten systems fulfill procurement roles including contract administration, data processing, acquisition management, and document control. They support the entire procurement business process implemented through various DoD programs producing specialized results. Each system provides stand alone functionality without interconnectivity to all the other systems. Equipment and software comprising these systems reflect a vast diversity of platforms, networks, and proprietary applications. As a result, any interaction between these systems and industry trading partners requires separate interconnection for each system.

4. SPS ARCHITECTURE

The goal of the SPS target architecture is to incorporate as much of the existing infrastructure as is feasible, practical, and economical. Open systems environment and the technology requirements for current commercial software packages influence this goal.

This document describes the SPS architecture developed to comply with the prevailing DoD standards listed in Appendix D. Of primary importance are the standards with guidance for software development, acquisition, and deployment within the DII and GCSS programs.

4.1 Architectural Design

The architectural design of the SPS, shown in Exhibit 4.1-1, illustrates a client/server architecture with distributed databases. Client/server technology generally means separating the user interface functions (the client) from the back-end processing and data storage (the server).

The SPS architecture in Exhibit 4.1-1 depicts three possible configurations of this client/server architecture. The center section shows the workstation or end user environment where no local or regional server is supporting the end user. The server at the DMC provides transaction processing and data storage for these end users. The two outer sections depict the scenarios where end users connect to a local or regional server. The end user may be with a local or regional server accessing the server through a LAN; accessing the server from an alternate location through a wide area network (WAN); or, accessing the server remotely via modem. In these scenarios, the user may also connect to a DMC for access to the Shared Data Warehouse (SDW), transmission of electronic commerce/electronic data interchange (EC/EDI) transactions, and backup support. Section 4.2 describes each connection scenario depicted in Exhibit 4.1-1.

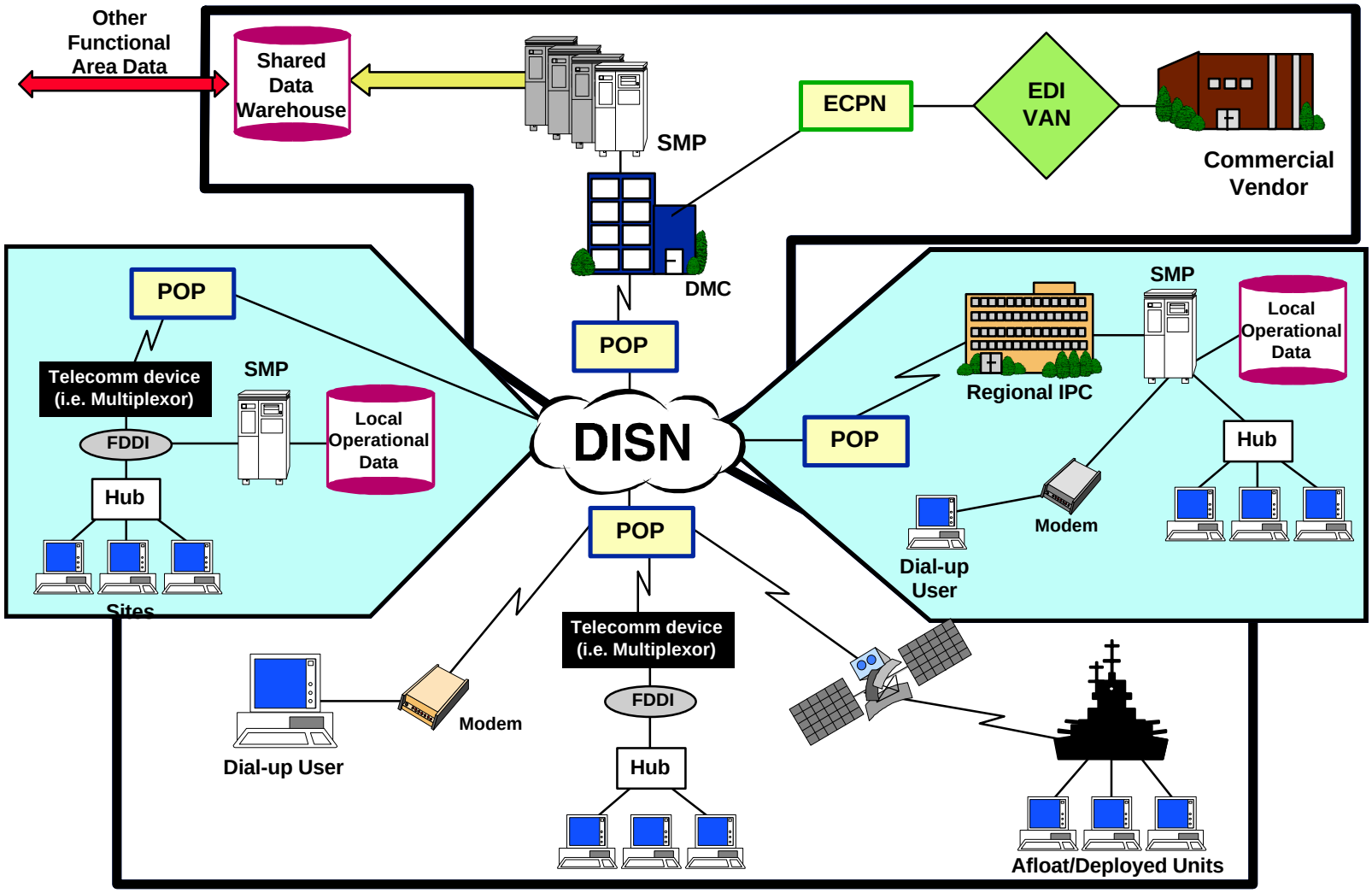

Exhibit 4.1-1: SPS Target Architecture

The architecture represented in this document represents the evolution of several architectural studies and reviews. The SPS Program Management Office (PMO) completed a full study of architecture alternatives for the Procurement Functional area in 1994 (*Comparison of Technical Architecture Alternatives for the Procurement Functional Area,* 25 October 1994). In this study, the SPS PMO evaluated five architecture alternatives against a set of criteria including performance, adaptability, survivability, training, operations, and security.

The architecture selected as the system's design framework was the Centralized with Replication alternative. This alternative is a regionally distributed client/server architecture in which a small number of sites contain a complete copy of the shared database. Multiple shared databases operate on multiple servers at different DMCs. The SPS PMO modified this alternative to incorporate existing local and regional servers and distributed databases. The local and regional servers provide local processing and data storage to the end user to reduce telecommunications traffic with the DMCs.

Each workstation client acquires data from one of the host databases, whether on a local, regional, or DMC server, and submits updates to the same host. Sites with local or regional servers can transmit updates to a DMC to ensure sustainability of shared data. Initial updates to the shared database will be via EDI transactions.

This open systems design facilitates modular enhancements, growth, and evolution throughout the life cycle of the SPS. The alternative described in this document offers an architecture not overly sensitive to changes in the total user population, changes in the location of those users, changes in hardware technology (including storage technology), or changes in communications technology. The architecture's response ability to change depends upon computer processing capacity and the telecommunications links that connect them. If either of these is inadequate, they may require additional modifications to prevent disruption of end user support. This modularity minimizes customer disruption as the system upgrades to accommodate changing requirements and the evolution of technologies.

By using the technical architecture described in this document, SPS ensures migration toward open systems goals of portability, interoperability, scalability, and common user interfaces. The SPS application requirement for standards compliance reinforces these open systems goals. Several government standards detail the open system goals.

- Technical Architecture Framework for Information Management (TAFIM)
- Defense Information Infrastucture Common Operating Environment (DII COE)
- Global Command and Support System (GCSS)
- Joint Tactical Architecture (JTA)

4.2 Connection Scenarios

As depicted in Exhibit 4.1-1, three possible connection scenarios exist for the end user in the target SPS architecture. Each end user receives processing and data storage support from at least one SPS server positioned in the local environment, at a regional processing facility, or at a DMC. Users within each connection scenario benefit from this architecture in varied ways. The

local and regional servers scenarios may utilize the DMC's ability to provide backup processing and data storage. The DMC processing scenario features duplication between DMC servers and the ability to reroute users experiencing a service interruption. The shared database always resides with at least one DMC.

4.2.1 Local Processing Scenario

Processing can occur locally as depicted in the site configuration shown at the left of Exhibit 4.1-1. Through the site's network(s), each workstation connects to the local server. The local server provides processing and stores the user data. The site can send contract data to the Shared Data Warehouse (SDW) at a DMC, and can send EC/EDI transactions to external trading partners or other Government communities via the electronic commerce processing node (ECPN) at a DMC. The site can also copy a full data backup to the DMC servers to ensure Continuity of Operations (COOP).

4.2.2 Regional Processing Scenario

Processing can occur regionally at a regional information processing center (IPC), shown at the right of Exhibit 5.1-1. Users at geographically separated bases may connect to a database at the regional IPC. As in the local scenario, sites may also send contract data to the SDW at a DMC, and can send EC/EDI transactions to external trading partners or other Government communities via an ECPN at a DMC. The regional can copy portions of their databases to the DMC server to ensure COOP.

4.2.3 DMC Processing Scenario

Processing can occur centrally at the DMC for sites without access to a local or regional server. Remote dial-up users, afloat users and deployed users can use the DMC processing alternative. The DMC server will maintain all data for these users in addition to providing the necessary processing support. The DMCs will provide COOP to sites using the DMC database for data processing and storage. These sites can also transmit contract data to the SDW via the DMC, and can send EC/EDI transactions to external trading partners or other Government communities via an ECPN at a DMC.

4.3 SPS Architecture Components

Each of the processing scenarios described above include varying subsets of the total set of architectural components. The primary architectural components of the SPS architecture include the user workstations, LANs, local and regional servers, DMC site servers, and the DISN. The host DoD component is responsible for providing and maintaining the SPS hardware and supporting environmental software described below, including the platform operating system, network operating system, and modems.

4.3.1 User Workstations

End users interact with the SPS at the workstation level. The user workstations supply the primary processing power of the SPS in the defined architecture. SPS can operate in a stand-alone environment supported by a Pentium or 486-based processor operating at 66Mhz or higher. Workstations may also get support from local, regional, and DMC servers. Communications

between areas employ LANs for on-site communications and the DISN for WAN connections. To support secure sites, the SPS can operate in a reduced capacity without DISN access in a stand-alone LAN mode.

4.3.1.1 User Workstation Hardware

The SPS contract defines the minimum desktop configuration for the end user workstation. This configuration comes from the minimum configuration specified by the "Department of Defense Personal Computer Policy Implementation Plan, FY 1995 - FY 2000," published by DASD (C3I Acquisition), 31 March 1995. The workstation includes a computer, either a portable laptop, notebook, or a personal computer, meeting the following minimum configuration:

- 66 MHZ processor clock speed,
- 36 integer SPECmark,
- 16 floating point SPECmark,
- 16 MB RAM, expandable to 32 MB
- 1 GB hard drive,
- two PCMCIA Type II slots, and
- two parallel and two serial ports.

4.3.2 Local Server

Some of the planned SPS sites use a local server that may or may not support one or more of the legacy systems. The target SPS architecture incorporates local servers to provide processing and data storage support to the end user.

4.3.2.1 Local Server Hardware

The typical local server configuration includes an environment with PCs networked to POSIX-compliant, 486-based machines, HP 9000s, RS6000s, or other similarly defined open system platforms. These local processing sites might also have symmetric multi-processing (SMP) platforms such as the HP9000 or Sun SPARCenter 2000.

4.3.2.2 Local Connectivity

Local sites consist of end user PCs connected over a LAN, fiber distributed digital interface (FDDI), or other type of LAN communications hub. These sites can connect via Transmission Control Protocol / Internet Protocol (TCP/IP) over the DISN to a DMC SPS server. DISN connectivity uses a DISN Point of Presence (POP) that may or may not be at the local site. If a local POP is not present, the user may lease or purchase a circuit to the nearest DISN POP.

4.3.3 Regional Server

The regional server is similar in configuration to the local server. However, the regional processing facility supports users co-located with the regional server or accessing the server remotely. In either case, the regional server provides processing and data storage capability to the end users.

4.3.3.1 Regional Server Hardware

SMP platforms support the regional servers. The possible regional server configuration includes an environment with PCs networked to POSIX-compliant minicomputer or platform servers.

4.3.3.2 Regional Connectivity

End users accessing a regional IPC can connect over a LAN, FDDI, WAN, or via modem. The regional facilities will have connectivity via TCP/IP over the DISN to a DMC SPS server. Typically, connectivity to the DISN uses a DISN POP located at the regional facility site.

4.3.4 Defense Megacenter

The DMCs perform several vital functions in the SPS environment. DMCs provide processing and data storage capabilities to the SPS end users who do not have access to a local or regional database. DMC facilities can also provide backup capability for local and regional servers. The DMC sites maintain electronic commerce processing nodes (ECPN). The DMC sites will also provide on-line transaction processing (OLTP) access to the SDW.

4.3.4.1 DMC Server Hardware

DISA chose the SMP platform as the near-term solution for SPS DMC processing. Recent studies determined that OLTP oriented systems, such as SPS, operate better in an SMP environment.

In addition to being OLTP oriented, the SMP platform supports EC/EDI transaction processing. This conclusion was the result of a recent study completed for DISA/D6 (Engineering). SPS depends upon EC/EDI transactions, which further supports the choice of SMP as the near-term solution for SPS processing.

4.3.4.2 DMC Connectivity

The DISN provides connectivity to and between DMCs. Section 6.2 discusses the DISN in detail.

4.3.4.3 Continuity of Operations

A primary benefit of the SPS architecture is sites using DMC services for processing survivability and data availability. These SPS users automatically gain the benefit of the DMC's COOP capability for data processing and storage. Sites with local or regional servers not accessing DMC services are responsible for providing COOP at the local level. DISA offers COOP support via the DMCs to sites on a fee-for-service basis. Section 5.5 discusses COOP strategies.

5. DATA

A driving force behind SPS development is the ability to create shared or common data. Before data is shared between systems or between communities, standardization must occur. This section describes legacy data, data formats, and servers processing and storing SPS data. The Shared Data Warehouse provides one method of sharing contract data between functional communities. This section concludes with an SPS data flow overview that incorporates the various components of the full SPS architecture.

5.1 Legacy Data

Past programs developed legacy procurement systems with varying levels of conformance to evolving data standards. SPS data standardization from the various legacy systems requires analysis and mapping to a structured data design to form the basis of the SPS application. The SPS vendor will provide a data migration plan and perform the migration/conversion of data from the legacy systems to SPS.

5.2 Data Formats

The SPS software provides electronic interfaces to external systems, including, but not limited to, materiel management and finance and accounting systems. To accomplish these interfaces, the SPS software accepts and outputs data in standard data element formats defined in the Defense Data Dictionary System (DDDS). For data transmitted in non-standard format, translation software will convert data to standard format on input, and to nonstandard format on output, to satisfy cross-functional interface data requirements. The SPS application also provides a method of reporting and resolving discrepant data or results.

To facilitate EDI, SPS software can originate or receive error-free flat files in ASCII text based on government-furnished data formats. The software extracts data to create user-defined files (UDFs) for originated transactions and imports data from incoming UDFs. These UDFs come from government implementation conventions conforming to American National Standards Institute (ANSI) X12, Version 3050 or newer.

5.3 Data Servers

Local, regional, DMC workstations provide the primary processing support for SPS users. Servers can maintain data at local, regional, or DMC sites. Each SPS server contains site specific operational data managed by a relational database management system (RDBMS) on that server.

The DMC servers offer additional functionality to the SPS end users beyond the direct support of users as described above. The DMC(s) support the SDW that serves as an SPS contract data repository to support corporate-level reporting and decision support requirements. All SPS sites have the option of uploading their transactions to a DMC site, thus ensuring the required COOP capability. Sites transmit EDI transactions directly to the EDI hubs, also maintained by the DMCs.

5.4 Shared Data Warehouse

The procurement community currently shares data with several functional activities, including contract payment. Currently, these activities do much of the data sharing manually, requiring multiple entries of data items. The target SPS architecture facilitates the sharing of contract data across functional areas by incorporating a shared data warehouse.

An SDW refers to a centralized collection of common data shared by multiple subject areas or functional domains in their business practices. An SDW allows the DoD buying, contract administration, and contract payment functions to share data. The use of the SDW with SPS will ultimately help reduce unmatched disbursements, as well as related problems, such as negative unliquidated obligations.

The SDW is in the early stages of implementation. The SDW resides at the Columbus, Ohio DMC. The warehouse resides in a Structured Query Language (SQL) compliant relational database management system. The SDW uses DoD standard data and is accessible to users and applications via the evolving DISN infrastructure. The initial population of the SDW is the government's responsibility. However, the SPS performs subsequent updates through EDI. The SPS will provide the ability to access, update, modify, and delete data in the data warehouse from deployed sites.

5.5 Continuity of Operations Strategies

Each site within the SPS program is responsible for continuity of operations. For those sites using the DMCs for data processing and storage, the DMCs provide the COOP. Sites using local or regional servers can provide their own COOP or take advantage of the DMCs COOP capabilities. Sites not already using the DMC for SPS processing can obtain COOP service on a fee-for-service basis.

Any regional or local site selecting the DMC COOP option can send transactions performed against user data in the operational database to the site’s designated DMC. This process ensures synchronization between the operational databases at any given point in time. The SPS architecture takes advantage of commercial database management systems (DBMSs) to achieve database synchronization. Asynchronous duplication, which performs the initial update (commit) of SPS data to the primary data server and subsequently duplicates the update to the designated DMC backup site(s), maintains database integrity for user data. Asynchronous duplication can occur in real-time or batch modes. Asynchronous duplication, as opposed to a two-phased commit approach, essentially achieves the same synchronization level between databases without a total dependence upon the databases’ availability to commit any single transaction.

Communications or hardware failures at any one of the sites will not affect end user transactions. In the event of a hardware or catastrophic failure, the SPS application reroutes client requests to a local, regional, or DMC server. This rerouting may occur transparently to the SPS end user or may be at the SPS end user's option. The application level implements the fault-tolerant capability described here. In this implementation, the SPS application assigns primary and alternate IP addresses to each SPS end user transaction. In the event that the primary SPS server becomes unavailable, the application re-submits SPS transactions to the alternate IP address of the backup

DMC site. After the primary SPS server becomes available again, the primary and secondary databases resynchronize.

The SPS vendor identifies the method of maintaining identical databases. The solution must provide notification and resolution capability in the event that any non-synchronized data exists. The application also contains the logic for routing transactions. It must respond to a variety of error conditions. The application can resubmit or reroute transactions as needed based on the response. The application must also resolve data integrity issues without unnecessarily limiting data access.

5.6 SPS Data Flow

This section provides an SPS data flow overview through the architecture described in this document. Exhibit 5.6-1 shows the data flow for a site with a local server. The basic flow is the same for each connection scenario and proceeds as follows.

The user transmits a request for data from a workstation to the primary server, whether local, regional, or DMC. The server retrieves the requested data from the Local Operational Database and transmits it to the requesting end user. The user may then update the data or generate new transactions. The server then saves the transaction at the Local Operational Database on the user's primary server. If the transaction contains contract data, the Shared Data Warehouse may also save it. If the transaction contains EC/EDI data, the server also transmits it through an ECPN to an external EDI value added network (VAN), then directs it to the commercial environment or government address as appropriate.

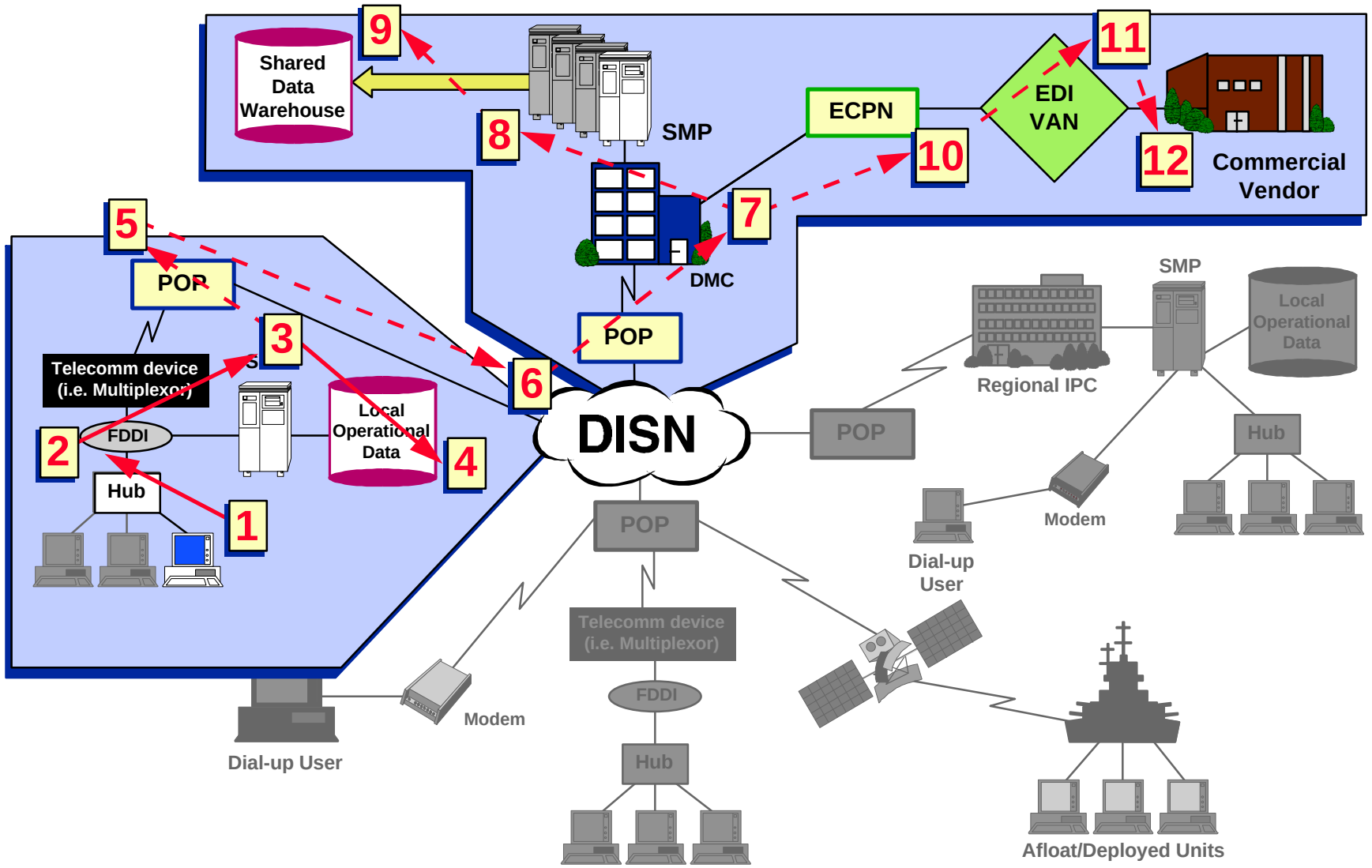

Exhibit 5.6-1: SPS Data Flow

6. SPS INFRASTRUCTURE

The SPS application can not exist independently. SPS is a functional application within the scope of the DII, and more specifically, the GCSS, using the DISN as its telecommunications infrastructure. The SPS integrates each of these programs. They play an important role in defining the SPS.

The DII provides information management capabilities to all mission areas of the DoD, and basically described as a globally distributed user-driven infrastructure. The DII contains two major systems: The Global Command and Control System (GCCS), and the Global Combat Support System (GCSS). GCCS implements the C4I For the Warrior concept. GCSS provides warfighting support functions, such as logistics and transportation. SPS is one of the initial systems deploying within the scope of GCSS.

All systems implemented within the scope of the DII support and receive support from the various levels of the DII framework. The DISN components support information transport services, including EC/EDI. The DMS provides the infrastructure for secure, accountable, reliable writer-to-reader messaging.

The following sections describe the elements of the DII in further detail and relate several of the DII systems or programs to SPS and the DII framework.

6.1 The Defense Information Infrastructure (DII)

The DII Strategic Architecture defines a computing and communications environment to support the transportable information requirements of the warfighter. The DII objective is to ensure the availability of information, regardless of the physical location of its end users, resulting in a "plug and play" capability. DoD mission support systems, such as the SPS, must support this capability. The DII is a distributed, heterogeneous computing environment characterized by a common operating environment (COE) processing at DMCs, sustaining bases, higher echelons of command, and the end user desktop. The DII supporting components include the computing, security, communications, management, and COE architectures. Integrating these components into an overall architecture strategy ensures an interoperable, scaleable, and secure environment for DoD applications and end users. The DII Master Plan, version 4.0, 26 April 1996, serves as an implementation and integration blueprint for elements within the DII scope.

6.1.1 DII Scope

The current DII comprises many elements, as shown in Exhibit 6.1-1. These elements are a mixture of components, services applications, and capabilities. Together, they indicate the scope of the DII. Enterprise integration efforts bring these elements together. The DII elements and their relationships continue to change as the DII evolves.

The DII elements build on and include a foundation of integration and technology support elements. The underlying technical infrastructure of the DII includes the DISN communications base; the DMCs for handling major information system processing and maintenance; and the DII

control concept to manage the DII network and systems. These elements interface with and support the base-level and tactical infrastructure.

DII functional applications get support from shared data, services, and technologies, all of which rely on the DII's technical infrastructure. The DII further supports functional applications through information warfare and associated information security to protect DII information assets. The DII supports interoperability of applications between DoD components and functional areas through the use of shared data and value-added services, such as EC/EDI and messaging. The COE and its support of cross-functional and cross-component integration provide technology solutions integrated with the value-added services. The COE provides common services and enables execution and integration of joint and service mission applications.

The functional applications drive the evolution of the DII. These applications include all DoD mission areas: Command and Control (e.g., GCCS), including tactical applications; Intelligence (e.g., the DoD Intelligence Information System (DoDIIS)); and Mission Support (e.g., the Depot Maintenance Standard System). The SPS application fits into the DII architecture at this level.

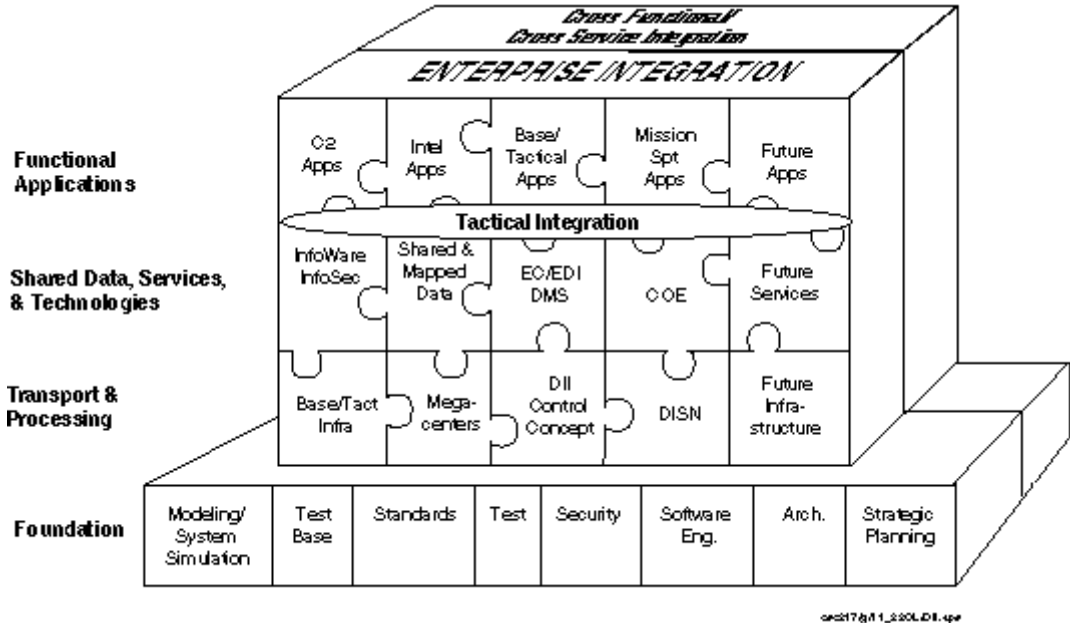

Exhibit 6.1-1: Scope of the DII

6.1.2 DII Computing

The DII computing environment is a distributed, heterogeneous environment implemented by using products based on the Open System Foundation (OSF) distributed computing environment (DCE). New DoD applications need to support the OSF DCE framework to facilitate the sharing of DoD computing resources and integration with other DCE-compliant applications. Object request broker (ORB) use achieves integration with non-compliant legacy applications. DoD will use the ORB that complies with the common object request broker architecture (CORBA). Remote procedure call (RPC) use implements DCE processing. OSF distributed file system (DFS) services support transparent access to data. TAFIM-compliant platforms and compliance with the DII COE enable portability and interoperability of the SPS across hardware platforms.

Processing at local installations, regional IPCs, and DMCs must support DII computing. DII applications may process at one or more of these levels, which DII control centers supporting the local, regional, and global levels manage. DISN provides the communications necessary for the integration and management of the DII components. A mix of RISC-based Unix and X-terminal workstations and DOS (CISC)-based platforms characterize the End User Desktop.

6.1.3 DII Communications

DII communicates internally via the DISN. The DISN is the DoD's consolidated, worldwide, enterprise-level telecommunications infrastructure. As the DISN infrastructure evolves, it provides information transport services that support sea, air, and ground mobile forces.

The DISN relies upon services of the broadband integrated services digital network (BISDN) and ATM/SONET technologies. DISN communication protocols use the Open Systems Interconnection (OSI) connectionless network protocol (CLNP) and Internet protocol (IP) suites and consist of three network layer services:

- Nonsecure (unclassified but sensitive) IP router network (NIPRNET),
- Secret IP router network (SIPRNET), and
- Top secret/sensitive compartmented information IP router network (TS/SCI)

Other protocols require conversion to or encapsulation within the IP or CLNP protocol. DISN POP routers accept IP or CLNP services.

The current DISN is a consolidation of the nine major networks operated by the military departments and supports both packet (X.25) and circuit switched networks. DISN will phase out X.25 services as users' transition to the DISN IP router layer. The maximum bandwidth available to DISN users are T1 circuits (1.544 Mbps). Near term plans call for T3 circuit speeds (45 Mbps), with SONET (>100 Mbps) planned for future years.

The DISN will evolve into a worldwide integrated and interoperable DoD common user infrastructure, with an architecture transparent to users and built on the principle of an open systems design. These capabilities will evolve through a combination of DISN communication services, DISN value-added information system services, and engineering consultative services.

6.1.4 DII Common Operating Environment

The DII COE provides a set of integrated support services for mission area application software and a corresponding software development environment. The COE provides architecture principles, guidelines, and methodologies that assist in mission application software development by capitalizing on the infrastructure support services. The COE components include support application services, application platform services, and application platform cross-area services identified by the DoD Technical Reference Model in the TAFIM, Volume 2.

The DII COE design supports an evolutionary development/migration strategy. To support DII evolution, the DII applications and services divide into three information application and service levels: (1) functional application domains, such as mission support applications; (2) value-added services, such as messaging and information discovery capabilities; and (3) underlying enabling services, such as high speed networks and global directories. These levels correspond to the mission applications, support applications, and platform services in TAFIM, Volume 2. The DII COE focuses on the value-added services and the underlying enabling services to support functional application needs.

Value-added services or support applications are common services for use across individual or multiple functional application domains. These services offer standard programmer interfaces to the mission area application developers. The application platform services area provides a standard set of services to support system interoperability objectives. The DII COE implements the enabling and value-added services on which the mission areas rely.

The DII COE design relies on the use of multi-tiered (e.g., client/server) concepts and distributed computing technology. The design consists of a hardware and software infrastructure that supports interoperability among command and control, intelligence, and mission support applications. In addition, the COE specifies a target profile of standards and services, consistent with the TAFIM.

Accessing the DII services requires a set of application program interfaces (APIs) for the DII. APIs from mission area COEs, such as those being developed for the GCCS, augment the APIs for the enabling and value-added services. Exhibit 6.1-3 shows a conceptual view of the DII COE.

The Defense procurement community will migrate to a COE through which users can access shared services via standard means. The DoD views DII COE as a common denominator, achievable regardless of mission area. The COE provides common support services available to all of the mission areas and enables execution and integration of joint and service mission applications. As the list of services offered by the DII COE evolves, revision occurs. The DII COE, together with approved common standards for integration of the mission area applications, supports legacy and migration applications as they evolve to the goal DII architecture.

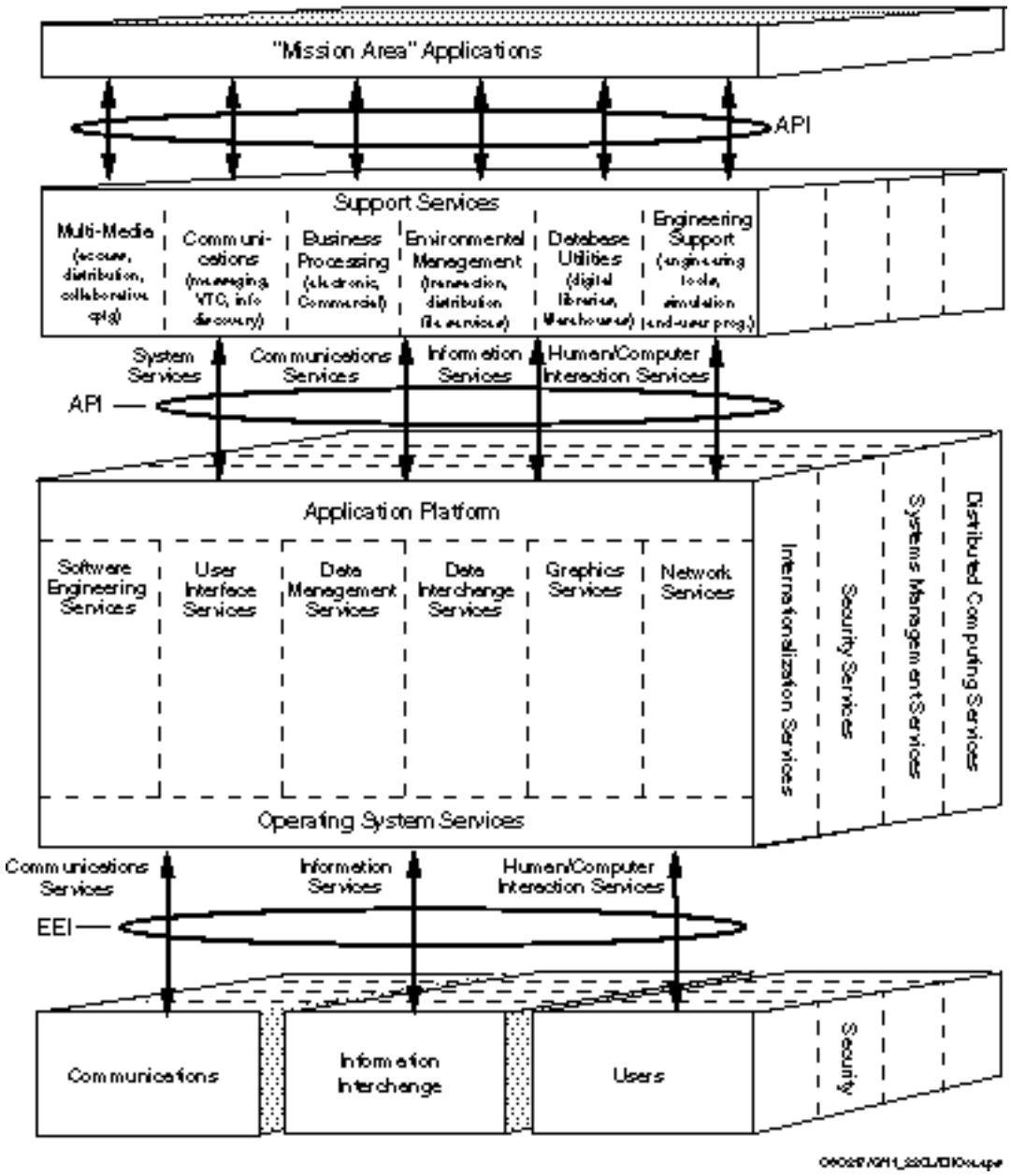

Exhibit 6.1-3: Conceptual View of the DII COE

6.2 Global Command and Support System (GCSS)

The Implementation Plan for the GCSS Initiative defines the GCSS as a demand driven, joint Warfighter focused initiative to accelerate delivery of improved combat support capabilities. GCSS is not an acquisition program; it is an initiative for interfacing and integrating DoD-wide Service/Agency sponsored Combat Support Systems. GCSS provides the common environment and shared infrastructure required to rapidly deploy integrated combat support capabilities for the Warfighter. The GCSS provides interoperable processing and communications by integrating combat support applications, databases, and commercial-off-the-shelf hardware and software through common operating and data environments. In conjunction with other DII elements including GCSS, DISN, Defense Messaging System (DMS), DMCs and CINC/Service/Agency projects, GCSS provides the information technology capabilities required to move and sustain joint forces. The GCSS fielding is incremental to match increasing user communities and the addition of new products to the common operating and data environments. The primary focus of GCSS is the integration of commercial-off-the-shelf information technology services with combat support applications and databases. The SPS program conforms with this goal and is one of the initial systems planned for fielding within the scope of the GCSS.

6.3 Defense Information Systems Network (DISN)

The DISN is a critical element in the DII. It provides a transparent, integrated global network supporting data, voice, image, and video services. The DISN is an evolving system that will develop into a worldwide integrated and interoperable DoD common user interface, with an architecture transparent to users and built on the principle of an open systems design. The near-term plan for DISN is the integration of the current network equipment of a variety of architectures.

The DISN serves as the telecommunications backbone of the SPS architecture. The DISN supports telecommunications between remote SPS end users and SPS servers; interprocess communication and duplication of data between DMC, regional, and local site servers; and the transmission of EDI transaction sets between the SPS servers and ECPN. Typical end-user connectivity to the DISN uses a DISN circuit connecting the sustaining base LAN or mobile unit (satellite) to a POP. SPS end users share telecommunications bandwidth on the DISN circuit to the DISN POP with the end users of other DoD applications. The DISN provides the service through which SPS end users, DMCs, EDI hubs, and DII control centers communicate and share information.

The DISN design integrates the distinct systems that currently comprise the DII into an infrastructure transparent to its users, facilitates the management of information resources, and responds to national security and defense needs under all conditions in the most efficient and cost-effective manner. The design requires flexibility to a constantly changing environment and responsiveness to the present and emerging requirements and needs of the customers.

6.4 EC/EDI

One specific use of the communications backbone provided by the DISN is the transmission of EC/EDI transactions. SPS relies on EC/EDI transactions for communication with entities outside the government procurement community (i.e., commercial vendors) and in certain instances within the government procurement community (i.e., SDW). SPS provides the capability for EDI transactions' transmission directly to and from the ECPN residing at the DMC sites. Sites transmit EDI transactions to the ECPN over the DISN. The DMC transmits the transactions through value added networks to the commercial community. The procurement community sends EDI transactions into the SPS environment via the same processes. Exhibit 6.3-1 illustrates the DoD EC/EDI Infrastructure.

The first section of the diagram displays examples of the functional proponents who make use of the EC/EDI technology. The Procurement/Contract Administration functional communities access the EC/EDI infrastructure through the SPS.

The center section of the diagram shows DISA's responsibility within the EC/EDI infrastructure. The EC/EDI gateways are hardware, software and communications platforms providing a single point of entry from one or more AISs to the network entry point. The gateways provide translation of ANSI X12 transactions to user defined files. The ECPN serve as "store and forward" collection points ensuring broad internal communications capabilities.

The final section of the diagram depicts the industry (non-DoD) environment. The VANs are public or private packet-switched networks that provide a variety of services and allow trading partners to have one communications environment.

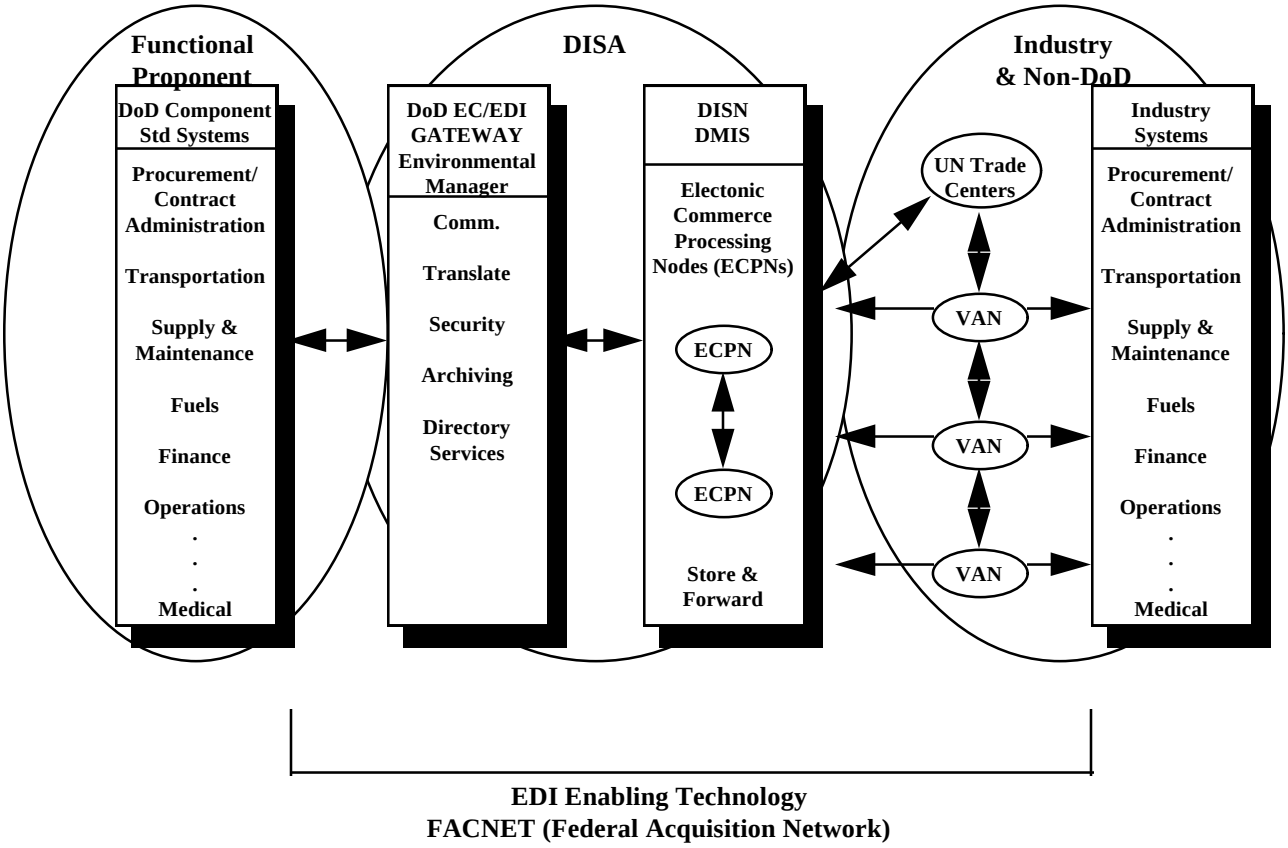

Exhibit 6.4-1: DoD EC/EDI Infrastructure

6.5 Defense Message System (DMS)

DMS is an electronic messaging system providing a secure, reliable, accountable, and responsive writer-to-reader messaging service to all DoD users. DMS also deploys a worldwide directory system used to store and distribute users' public security credentials electronically. DISA manages the worldwide DMS infrastructure. MISSI technology protects management traffic between management centers and DMS infrastructure components. MISSI technology will employ future evolutionary enhancements as they become available to provide additional security measures in a classified environment.

DMS is the first major deployment of MISSI technology. It is the program that the NSA used to baseline the MISSI requirements. DMS plans include the employment of the same MISSI technology as the other core DII programs.

6.6 Multilevel Information Systems Security Initiative (MISSI)

Each DII core program employs a variety of security products being developed under the NSA MISSI and approved by the National Computer Security Center. Commercial-off-the-shelf

security products may also be implemented where they complement or enhance MISSI product capabilities.

MISSI products provide the user with a wide range of information security capabilities, including services that insure data transmissions are neither accidentally corrupted nor deliberately compromised by a third party prior to receipt. Strong identification and authentication of both the message originator and message recipients support enforcement of the local access control policies. They also provide necessary protection of electronic messages from unauthorized disclosure of the message contents. In addition, the MISSI products support a non-repudiation security service wherein one party involved in a communication cannot deny involvement after the fact. These products also support the collection of audit information.

The FORTEZZA card is the primary MISSI hardware for the individual user. FORTEZZA provides effective authentication of the user's identity and access privileges, confidentiality, data integrity, non-repudiation services, and support for various workstations operating systems.

SPS security planning centers around MISSI security products, including the FORTEZZA solution that capitalizes on enhanced security services to insure data integrity while in transit during a user-to-host data exchange. The FORTEZZA-equipped host application system also insures data integrity during processing and in storage in the SPS information domain. Use of FORTEZZA provides assurance that procurement/contracting data generated from SPS to the EC/EDI process receives protection from its' source of origin. However, if FORTEZZA is not available and accepted at the time of deployment, SPS will use the current NSA-approved MISSI product to ensure data protection and confidentiality.

7. CONCLUSION

The SPS Infrastructure/Architecture Document provides a technical reference for the Procurement community. This document supports planning, documentation, and other related efforts supporting the Major Automated Information System Review Council (MAISRC) requirements.

This is a living document revised as needed to reflect updates in the program strategy, progress, technological advances, and other modifications as deemed necessary by the SPS PMO.

Appendix A:

Glossary

Term	Definition
Application Program Interface (API)	(1) The interface, or set of functions, between the application software and the application platform. (2) The means by which an application designer enters and retrieves information.
Asynchronous	A communications method in which data are sent as soon as they are ready, as opposed to methods in which data are sent at fixed intervals; requires start and stop bits to separate characters.
Asynchronous Transfer Mode (ATM)	A data transfer mode in which a multiplexing technique for fast packed switching in Consultative Committee for International Telephone and Telegraph (CCITT) broadband Integrated Services Digital Network (ISDN) is used. This technique inserts information in small fixed-sized cells (32-120 octets) that are multiplexed and switched in a slotted operation, based upon header content, over a virtual circuit established immediately upon a request for service.
Automated Information System (AIS)	Computer hardware, computer software, telecommunications, information technology, personnel, and other resources that collect, record, process, store, communicate, retrieve, and display information. An AIS can include computer software only, computer hardware only, or a combination of the above.
C2	Business sensitive but not classified data
Client / Server	A database management system involving stored databases (servers) and users at connected sites (clients). Most common database management system in use.
Clock speed	The internal processing speed of the computer
Common Operating Environment (COE)	A scheme whereby all computers operating within the same network or group utilize the same operating system in order to ensure portability and compatibility throughout the system.
Corporate Information Management (CIM)	A strategic collaborative management initiative to improve DoD performance and capture the benefits of the information revolution.
Data Integrity	Protection against unauthorized modification, insertion, and deletion. Example: Electronic funds transfer between banks requires protection against modification of the information.
Database	A stored set of records that can be sorted, queried, and modified.
Database Management System	Computer application program that accesses or manipulates the database.

Direct Connection	A Direct data link between a terminal and a host computer owned for exclusive use of the system
Electronic Commerce (EC)	End-to-end, paperless business environment that integrates electronic transfer and automated business system.
Fiber Distributed Data Interchange (FDDI)	An ANSI LAN standard physical access media which utilizes a token passing ring technique and supports data rates of 100 megabits per second.
File Transfer Program (FTP)	A TCP/IP application program used to transfer files from one computer to another. It is commonly used on the Internet.
Gateway	A device for converting one network's message protocol to the format used by another network's protocol. It can be implemented in hardware or software.
Graphical User Interface (GUI)	System design that allows the user to effect commands, enter into transaction sequences, and receive displayed information through graphical representations of objects (menus, screens, buttons, etc.).
Infrastructure, architecture	The set of hardware, telecommunications, and software present for a given system. Also the hardware configuration.
Internet	The collection of networks and gateways, including the MILNET and NFSNET, that use the TCP/IP protocol suite and function as a single, cooperative virtual network. The Internet provides universal connectivity and three levels of network services: unreliable, connectionless packet delivery; reliable, full duplex stream delivery; and application-level services like electronic mail that build on the first two. The Internet reaches many universities, government research labs, military installations, and dozens of foreign countries.
Internet Protocol (IP)	Standard that allows dissimilar hosts to connect to each other through the DDN.
Interoperability	(1) The ability of two or more systems or components to exchange and use information. (2) The ability of the systems, units, or forces to provide and receive services from other systems, units, or forces, and to use the services so interchanged to enable them to operate effectively together. The conditions achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users.
Leased Circuit	A data link owned by another party on which time is bought for connections
Legacy Environments	Legacy environments could be called legacy architectures or infrastructures and as a minimum consist of a hardware platform and an operating system. Legacy environments are identified for phase-out, upgrade, or replacement. All data and applications software that operate in a legacy environment

	must be categorized for phase-out, upgrade, or replacement.
Legacy Systems	Systems that are candidates for phase-out, upgrade, or replacement. Generally legacy systems are in this category because they do not comply with data standards or other standards. Legacy system workloads must be converted, transitioned, or phased out (eliminated). Such systems may or may not operate in a legacy environment.
Local Area Network (LAN)	A data network, located on a user's premises, within a limited geographic region. Communication within a local area network is not subject to external regulation; however, communication across the network boundary may be subject to some form of regulation.
Massively Parallel Processing	A parallel computer with at least one hundred processors. These processors are capable of running many jobs simultaneously or utilizing the processing power to reduce the running time of a single job.
Migration Systems	An existing AIS, or a planned and approved AIS, that has been officially designated to support common processes for a functional activity applicable to use DoD-wide or DoD Component-wide. Systems in this category, even though fully deployed and operational, have been determined to accommodated a continuing and foreseeable future requirement and, consequently, have been identified for transitioning to a new environment or infrastructure. A migration system may need to undergo transition to the standard technical environment and standard data definitions being established through the Defense IM Program, and must "migrate" toward that standard. In that process, it must become compliant with the Reference Model and the Standard Profile. A system in this category may require detailed analysis that involves a total redesign, reprogramming, testing, and implementation because of a new environment and how the "users" have changed their work methods and processes. The detailed analysis may identify the difference between the "as is" and the "to be" system.
Military Network (MILNET)	The Defense Data Network unclassified operational military network.
Network	A system of connected computers.
On-line Transaction Processing (OLTP)	A method of processing transactions in real-time rather than in batch mode or off-line
Open System	A system that implements sufficient open specifications for interfaces, services, and supporting formats to enable properly engineered applications software: (1) to be ported with minimal changes across a wide range of systems, (2) to interoperate with other applications on local and remote systems, and (3) to interact with users in a style that facilitates user portability.

Operating System	A group of program operating under the control of a data processing monitor program. It manages such functions as memory, processing tasks, and interprocess communications in a computer system.
Platform	A computer system (e.g., PC, mainframe)
Plug and Play	The ability to plug in the computer, load the software, and be able to access information without intermediate steps
Portability	(1) The ease with which a system or component can be transferred from one hardware or software environment to another. (2) A quality metric that can be used to measure the relative effort to transport the software for use in another environment or to convert software for use in another operating environment, hardware configuration, or software system environment. (3) The ease with which a system, component, data, or user can be transferred from one hardware or software environment to another.
Portable Operating System Interface for Computer Environments (POSIX)	An IEEE standard operating system interface defining the external characteristics and facilities required to achieve the portability of applications at the source-code level.
Protocol	A set of rules for communication
Relational Database Management System (RDBMS)	A database management system used in a relational database setting.
Router	Generically, any machine responsible for making decisions on which path out of several different paths.
Scalability	The ability to use the same application software on many different classes of hardware/software platforms from personal computers to super computers (extends the portability concept). The capability to grow to accommodate increased workloads.
Symmetric Multi Processing	A SMP is a tightly coupled system in which the processors share common main memory and disks. SMP systems increase performance by offloading operating chores from the primary processor to additional processors.
Synchronous	A type of system in which the send and receive instruments are operating continuously at substantially the same frequency and are maintained in a desired phase relationship; a method of packing bits inside a block with regular synchronized timing, negating the need for sending shared and stop bits between characters to achieve a higher data rate.
TCP/IP Gateway	A device, or pair of devices, that interconnects two or more networks or subnetworks, enabling the passage of data from one (sub)network to another. In this architecture, a gateway contains an IP module and, for each connected subnetwork, a subnetwork protocol (SNP) module. The routing protocol is used to coordinate with other gateways. A gateway is often

	called an IP router.
Technical Architecture Framework for Information Management (TAFIM)	The TAFIM is a set of documents produced by DISA for the OSD to guide DoD information systems toward an open systems architecture. It provides the services, standards, design concepts, components, and configurations that can be used to guide the development of technical architectures that meet specific mission requirements.
Technical Reference Model (TRM)	The document identifies a target framework and profile of standards for the DoD computing and communications infrastructure.
Value-Added Network (VAN)	Communications network that transmits, receives, and stores EDI messages for EDI trading partners.
Wide-Area Network (WAN)	A public or private computer network serving a wide geographic area.
X.25	Recommendations developed by CCITT that define a protocol for communication between packet-switched public data networks and user devices in the packet switched mode.

Appendix B:

Acronym List

ADP	Automated Data Processing
AFMCS	Air Force Material Command Suite
AIS	Automated Information System
AMIS	Acquisition Management Information System
ANSI	American National Standards Institute
APADE	Automation of Procurement and Accounting Data Entry
API	Application Program Interface
ASCII	American National Code for Information Interchange
ATM	Asynchronous Transfer Mode
BCAS	Base Contracting Automation System
BISDN	Broadband Integrated Services Digital Network
BOSS	Base Operating Supply System
CCSS	Commodity Command Standard System
CINC	Commander In Chief
CISC	Complete Instruction Set Computing
CIM	Corporate Information Management
CLNP	Connectionless Network Protocol
COE	Common Operating Environment
COOP	Continuity of Operations
CORBA	Common Object Request Broker Architecture
CPU	Central Processing Unit
DBMS	Database Management System
DCE	Distributed Computing Environment
DDDS	Defense Data Dictionary System
DFS	Distributed File System
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DLA	Defense Logistics Agency
DMA	Defense Mapping Agency
DMC	Defense Megacenter
DMS	Defense Messaging System
DoD	Department of Defense
DoDIIS	DoD Intelligence Information System
DPACS	DLA Pre-Award Contracting System
DPCSC	Defense Procurement CIM Systems Center
EC	Electronic Commerce
ECPN	Electronic Commerce Processing Node
EDI	Electronic Data Interchange

FDDI	Fiber Distributed Digital Interface
FTP	File Transfer Protocol
GB	GigaByte
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GUI	Graphical User Interface
IP	Internet Protocol
IPC	Information Processing Center
IS	Information Systems
ITIMP	Integrated Technical Item Management Procurement
LAN	Local Area Network
Kbps	Kilobits per second
MAISRC	Major Automated Information System Review Council
MB	MegaByte
MHZ	MegaHertz
MILSCAP	Military Standard Contract Administration Procedure
MILSTRIP	Military Standard Requisitioning Issue Procedure
MISSI	Multilevel Information Systems Security Initiative
MOCAS	Mechanization of Contract Administration Services
NIPRNET	Nonsecure IP Router Network
NSA	National Security Agency
OLTP	On-Line Transaction Processing
ORB	Object Request Brokers
OSF	Open System Foundation
OSI	Open Systems Interconnection
PADDS	Procurement Automated Data and Document System
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
PMO	Program Management Office
PMP	Program Management Plan
POP	Point of Presence
POSIX	Portable Operating System Interface for Computer Environments
PR	Purchase Request
R&D	Research and Development
RAM	Random Access Memory
RDBMS	Relational Database Management System
RISC	Reduced Instruction Set Computing
RPC	Remote Procedure Calls
SAACONS	Standard Army Automated Contracting System
SDW	Shared Data Warehouse
SIPRNET	Secret IP Router Network
SMP	Symmetric Multi-Processing
SONET	Synchronous Optical Network
SPS	Standard Procurement System
SQL	Structured Query Language

TAFIM	Technical Architecture Framework for Information Management
TCP/IP	Transmission Control Protocol / Internet Protocol
TRM	Technical Reference Manual
TS/SCI	Top Secret/Sensitive Compartmented Information IP Router Network
UDF	User Defined File
VAN	Value Added Network
WAN	Wide Area Network
WWW	World Wide Web

Appendix C:
References

Comparison of Technical Architecture Alternatives for the Procurement Functional Area, 25 October, 1994.

Cross-Functional Analysis Baseline, Draft, 7 July 1995.

Defending the Defense Information Infrastructure (DII): DISA's Vision & Strategy for Defensive Information Warfare; Col Ken Ritchhart, DISA-D3, 25 April 1995.

Defense Information Infrastructure (DII) Common Operating Environment (COE) Baseline Specifications, Version 3.0, 31 October 1996.

Defense Information Infrastructure (DII) Common Operating Environment (COE) Distributed Computing Environment (DCE), 30 September 1996.

Defense Information Infrastructure (DII) Common Operating Environment (COE), Integration & Runtime Environment Specification, Version 2.0, 23 October 1995.

Defense Information Infrastructure (DII) Common Operating Environment (COE) Programmer's Manual, Version 3.0, 31 October 1996.

Defense Information Infrastructure (DII) Common Operating Environment (COE) Programmer's Reference Manual, Version 3.0, 31 October 1996.

Defense Information Infrastructure (DII) Master Plan, Version 4, 26 April 1996.

Defense Information Infrastructure (DII) Strategic Enterprise Architecture, Coordination Draft, 16 February 1995.

Department of Defense Joint Technical Architecture (JTA), Version 1.0, 22 August 1996

Department of Defense Personal Computer Policy Implementation Plan, FY 1995 - FY 2000, DASD (C3I Acquisition), 31 March 1995.

Department of Defense Technical Architecture Framework for Information Management (TAFIM); Volume 2: Technical Reference Model and Standards Profile Summary, Version 2.0, 30 June 1994.

Department of Defense Technical Architecture Framework for Information Management (TAFIM); Volume 3: Architecture Concepts and Design Guidance, Version 2.0, 30 June 1994.

GCCS Baseline Common Operating Environment, 28 November 1994.

Global Command and Control System Integration and Runtime Specification, Version 2.0 Draft, August 1995.

Implementation Plan for Global Combat Support System (GCSS) Initiative, 7 December 1995.

Information Paper on Symmetric Multiprocessors (SMP) and Massive Parallel Processors (MPP) for EC/EDI application for RADM John Gauss; Mr. Ken Linker, Center for Software, 22 August 1995.

Multilevel Information Systems Security Initiative (MISSI), National Security Agency Information Systems Security Office, October 1996.

Report on the Standard Procurement System (SPS) Migration Strategies, Version 3.0, DPCSC, 5 February 1997.

Shared Procurement Data Warehouse Concept of Operations, DLA Systems Design Center (DSDC), 22 March 1996.

Shared Data Base White Paper, Boeing Information Services, 30 June 1995.

Shared Data Warehouse (SDW) Architecture Planning Paper (Draft), 8 December, 1995

Standard Procurement System (SPS) Program Management Plan, MAISRC Milestone I, 30 June 1995.

Standard Procurement System Migration Project Transition Plan, Boeing Information Services, 28 May 1996.

Standard Procurement System Migration Project Telecommunications and Interoperability Plan, Boeing Information Services, 21 May 1996.

Standard Procurement System Migration Project Integration Plan, Boeing Information Services, 28 May 6.

Standard Procurement System (SPS) Contract, 23 August 1996.

Standard Procurement System (SPS) System Security Plan (working copy), 16 January 1997.

Appendix D:
Standards

The architecture described within this document has been developed in compliance with the prevailing DoD guidance directing open systems platforms. In addition, there are several standards with which the SPS application must be compliant. These standards are referenced throughout this document and are summarized briefly below.

1. Technical Architecture Framework for Information Management (TAFIM)

SPS will be compliant with all TAFIM standards. TAFIM characterizes an information system as composed of data, mission-specific applications, and a technical infrastructure (as described in TAFIM Vol. 2, The TRM) consisting of support applications, application platforms, and communications networks.

2. Portable Operating System Interface for Computer Environments (POSIX)

All versions of the SPS application must be capable of operating in a POSIX-compliant environment. POSIX is a standards based architecture for communications and security environments.

3. Global Command and Control System Integration and Runtime Specifications

The SPS application should make use of the guidelines set forth in the Global Command and Control System Integration and Runtime Specifications (Version 2 Draft) dated August 1995. This document describes integration standards, software requirements, and, the process and tools developed for automated integration of GCCS software.

4. Global Command and Control System Baseline Common Operating Environment

The SPS application will incorporate the guidelines set forth in the Global Command and Control System Baseline Common Operating Environment dated 28 November 1994. This document defines a set of integrated support services that support the mission application software requirements and a corresponding software development environment, architecture principles, and methodology that assists in the development of mission application software by capitalizing on the infrastructure support services. This document also includes an appendix that identifies the standard application programmer interfaces (APIs) to the operating system.

5. Federal Acquisition Computer Network

The SPS application must meet the certification requirements for the Federal Acquisition Computer Network (FACNET), a government wide EC/EDI infrastructure. FACNET provides universal user

access with both national and international data formats. The FACNET gives an easily understood, common standard with which to use EC/EDI.

6. Application Implementors Guide and Cryptologic Interface Programmers Guide

The SPS software will protect system data through use of the FORTEZZA crypto-card in accordance with the Application Implementors Guide and Cryptologic Interface Programmers Guide issued by the National Security Agency.

7. Department of Defense Personal Computer Policy Implementation Plan, FY 1995 - FY 2000

The SPS software will be required to run on a minimally configured user workstation. This configuration is based on the SPS contract configuration statement which is based on the configuration contained herein. This minimum requirement is needed in order to ensure connectivity, operability, and functionality throughout the user community of SPS.

8. DII Master Plan

SPS will follow the guidance set forth in the DII master plan. The DII contains several levels including Functional Applications, such as SPS; Shared Data, Services, and Technologies, such as EC/EDI; Transport and Processing, such as DISN; and a Foundation level which includes standards, security, and the architecture of the system. All elements of this system are integrated under an enterprise integration framework for form the DII master plan.

9. DII COE Integration & Runtime Environment Specification

The SPS application will comply with the guidance provided by the DII COE Integration & Runtime Environment Specification. This document defines an approach for building interoperable systems, a collection of reusable software components, a software infrastructure for supporting mission area applications, and a set of guidelines and standards. The DII COE defines a foundation for building an open system.

10. Joint Technical Architecture (JTA)

The SPS application must comply with standards outlined in the JTA. The JTA identifies a common set of mandatory information technology standards and guidelines used in all new and upgraded C4I acquisitions across DoD. The JTA standards are for sending and receiving information, understanding the information, and processing that information. The JTA also includes a common human-computer interface and rules for protecting the information.

Integration Team Documents Page